(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 September 2003 (04.09.2003)

PCT

(10) International Publication Number
WO 03/073242 A1

(51) International Patent Classification[7]: G06F 1/00, H04L 29/06

(21) International Application Number: PCT/SE03/00341

(22) International Filing Date: 28 February 2003 (28.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/361,382 28 February 2002 (28.02.2002) US
60/337,059 1 May 2002 (01.05.2002) US

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET L M ERICSSON (PUBL)** [SE/SE]; S-126 25 Stochkholm (SE).

(72) Inventors; and

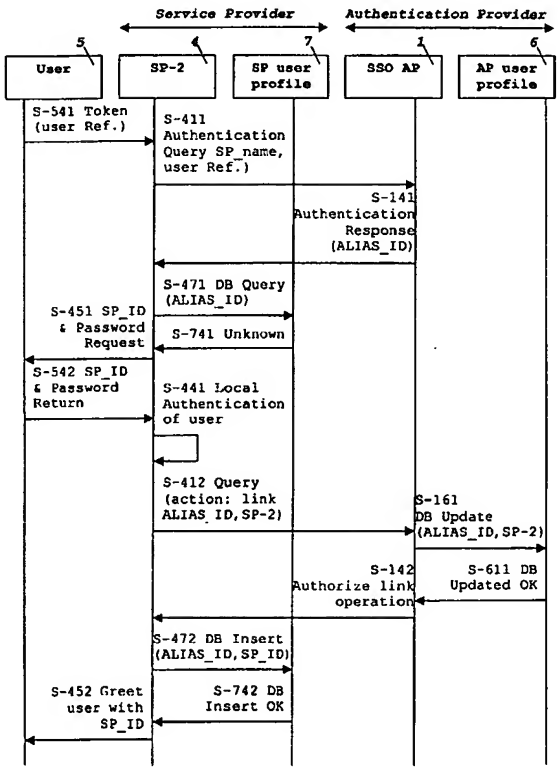
(75) Inventors/Applicants *(for US only)*: **BARRIGA, Luis** [SE/SE]; Pilotgatan 50, S-128 33 Skarpnäck (SE). **PARDO-BLAZQUEZ, Avelina** [ES/ES]; C/ Sombrerete nr. 5-2ª 3ª, E-28012 Madrid (ES). **WALKER, John, Michael** [GB/ES]; C/ Juan-Martin-El-Empecinado, 9-1C, E-28045 Madrid (ES). **DE GREGORIO, Jesús-Angel** [SE/SE]; C/ Hermanos Machado, nr. 4 P3 2°, E-28660 Boadilla del Monte-Madrid (SE).

(74) Agent: **BOESTAD, Karin**; Ericsson AB, Patent Unit Core Networks Kista, S-164 80 Stockholm (SE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR HANDLING USER IDENTITIES UNDER SINGLE SIGN-ON SERVICES



(57) Abstract: The invention provides a mechanism, in terms of means and method, for handling, provisioning and correlating a plurality of user's identities for a user in an automated manner between a single sign-On authentication provider and a number of service providers where the user accesses. Therefore, after a successful authentication of a user's authentication identity with the authentication provider, the authentication provider assigns an alias shared identity to the user, said alias shared identity being the uniquely exchanged identity between the authentication provider and the service provider to identify the user. The alias shared identity is linked at the authentication provider with the user's authentication identity and with an identifier of the service provider where the user accesses. The alias shared identity is linked at the service provider with the user's local identity which the user has for an account with the service provider.

WO 03/073242 A1

SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Method and apparatus for handling user identities under Single Sign-On services

FIELD OF THE INVENTION

[0001] The present invention generally relates to Single Sign-On services for a user having a plurality of user identities. More particularly, the invention pertains to means and methods for handling a plurality of user identities that a user may have under different service providers, while allowing a Single Sign-On authentication for the user.

BACKGROUND

[0002] The Internet is a growing network wherein services are provided by different organisations generally known as service providers. Many service providers allow users the possibility to have accounts with them. Indeed, depending on the service offered, it is often required to have an account at a given service provider. The access to a given service provider may require users to authenticate themselves towards the service provider. In other words, users must be able to prove who they are. This is most often achieved by providing an identity, namely a username, and a password. Once a user is authenticated, she or he is allowed to access a requested service as well as an account that the user may have at the service provider. In this context, a user's account is understood as personal and confidential information. At present, users may have a number of identities and passwords at different service providers, each couple identity/password being used to authenticate a user at a service provider.

[0003] The advent of Internet services has brought with them a new service that allows users to access said Internet services in an easy and convenient manner, the so-called Single Sign-On (SSO) service. The current principle behind Single Sign-On states that users shall be able to authenticate once and shall be given access to all their subscribed services that accept such level of authentication. Single Sign-On is an emerging service that enables users to access different service providers without requiring a particular user's authentication at each service provider. In other words, a user provides identity/password only once at a given service provider and the resulting authentication is valid for entrance to other service providers.

[0004] Conventional cellular operators, hereinafter referred to as Mobile Network Operator (MNO), make use of authentication services to grant subscribers accesses to voice and data services provided by such operators. As cellular operators move up in the value chain, they could leverage their mutual trust relationship with their own subscribers in order to play a new role of Authentication Providers for their respective subscriber population in emerging business models wherein service domain and authentication domain belong to different administrative entities. In this respect, an operator that is able to provide both accesses, namely IP connectivity and services, might additionally offer to its subscribers an "*access authentication SSO*" so that an authentication performed at the access domain may be a valid authentication in a service domain. Generally speaking, an Authentication Provider may belong to the same administrative domain as the Service Provider offering the service, or may be delegated to an external trusted party such as a cellular operator.

[0005] Single Sign-On (SSO) is thus based on trust. That is, a first service provider trusts another party, which in particular might be a second service provider carrying out a Single Sign-On (SSO) authentication, to authenticate a user who is accessing a site of said first service provider. The first service provider has no way of knowing whether or not said user already has an account with it and, if so, under which user identity. This occurs because the identity furnished by the user at an accessed site does not necessarily match the identity furnished during the Single Sign-On (SSO) authentication process. Indeed, if such user identity furnished during the SSO authentication process matches an existing user identity for the user at the accessed site of said first service provider, then direct access to related accounts may be granted, but this is merely a coincidence and can not be considered a valid mechanism within a generally applicable method.

[0006] The present invention is aimed to solve a more general case in which users are known under different identities for accounts scattered across the Internet, thus allowing a Single Sign-On (SSO) authentication provider to correlate user identities and the users making use of a user's preferred identity per each service provider as well as accessing a service provider in an anonymous manner despite performing a Single Sign-On (SSO) authentication.

[0007] A primary object of the present invention is the support of an appropriate mechanism, in terms of means and method, for handling, provisioning and correlating a plurality of user identities for a user in an automated manner between an SSO Authentication Provider, such as a Mobile Network Operator (MNO) or a first service provider capable of performing an SSO authentication, and a number of second Service Providers in order to allow each user

having a personalised access to its user's accounts at said second Service Providers.

RELATED ART

[0008] The international publication WO-200160013 shows a Single Sign-On process that allows a mobile user with a mobile phone or with a laptop to remotely access a remote server. This teaching only deals with SSO authentication for users in a mobile or cellular network by stressing role of a smart card. There is no support in this publication for handling, provisioning and correlating a plurality of user identities for a user in an automated manner between an SSO Authentication Provider and a number of Service Providers.

[0009] On the other hand, the international publication WO-200111450 just presents a Single Sign-On framework with a trust-level mapping to authenticate requirements for improving the security of information transactions over a number of networks. This teaching only deals with authentication in a generic SSO solution wherein there is no need for handling, provisioning and correlating a plurality of user identities for a user in an automated manner between an SSO Authentication Provider and a number of Service Providers.

[0010] Another significant instance of methods and system for Single Sign-On user access is described in the European patent application EP-1089516 to Grandcolas et al. wherein users may gain access to multiple web servers. This application describes how a user is authenticated at a first web server that allows the user to select a second web server offering a desirable service. When the user effectively selects the second web server, the first web

server constructs an encrypted authentication token, and transmits it to the second web server. The second web server authenticates the received token and allows the user to have a session at this second web server. Both first and second web server share, in accordance with this application, a sub-domain. That is, the scenario in this application is an instance where the Authentication Provider, namely the first web server, and the Service Provider, namely the second web server, both belong to the same administrative domain. Thereby, the teaching in this application cannot be applied to those scenarios where Authentication Provider and Service Provider belong to different administrative domains. Moreover, this approach can not be applied in scenarios where there is a need for handling, provisioning and correlating a plurality of user identities for a user in an automated manner between an SSO Authentication Provider and a number of Service Providers.

[0011] Another known solution nowadays under Single Sign-On services, and which is representative of a scenario where Authentication Provider and Service Provider belong to different administrative and commercial domains, is the Microsoft ® .NET Passport product (as described in http://www.passport.com and hereinafter simply referred to as ".NET Passport"). This product is intended to build up a broader Internet trust network with a common set of technical and operational guidelines open to organizations supporting the corresponding standards. However, this approach does not solve the problem of handling, provisioning and correlating a plurality of user identities for a user in an automated manner between an SSO Authentication Provider and a number of Service Providers, especially for user identities scattered throughout the Internet and for Service Providers not associated to ".NET Passport" or not following the corresponding standards.

[0012] A currently known approach, which may apply in an SSO scenario wherein a user makes use of different user identities for different service providers, assumes that a user has an agreement with an SSO Authentication Provider such as a Mobile Network Operator holding a subscription for said user. In this scenario, as Fig. 1 illustrates, an SSO Authentication Provider stores the following user information per user basis:

- one valid single sign-on identity that is used for authentication purposes (hereinafter AP_ID) and as entry key to access a given profile; and
- a number of specific user identities per service provider web site basis (each user identity hereinafter referred to as SP_ID), each SP_ID being accessed via the aforementioned AP_ID.

[0013] In this approach, the SSO Authentication Provider authenticates a user towards a number of service providers. The user provides an identity (AP_ID) and password to be authenticated once and accesses other web sites as an authenticated user. If the user has other user identities with other Service Providers the user must manually input the list of these other identities (SP_ID-1, SP_ID-2) at the trusted SSO Authentication Provider. In this way, each Service Provider addresses a user with the identity said user is known locally at the Service Provider and not with the AP_ID used for being authenticated.

[0014] A first disadvantage from this approach is that users, or rather the SSO Authentication Provider owner, have to manually input a number of user identities that the user has with other Service Providers at the trusted SSO Authentication Provider. That is, there is no automated method and corresponding means to provide a reliable solution for inter-domain provisioning and for handling

identity related information of an end-user in a Single Sign-On (SSO) context. Inter-domain may refer in this context to interactions between an SSO Authentication Provider, such as for example a Mobile Network Operator (MNO), and a number of Service Providers (SP-1, SP-2) accessible over the Internet. In this respect, no solution currently exists that allows different user identities belonging to different domains to be automatically linked and provisioned by both the SSO Authentication Provider and a Service Provider.

[0015] An important drawback from the above approach is the fact that an SSO Authentication Provider domain stores, and thus knows, a number of user identities for each user with different Service Providers, the latter belonging to other domains. This drawback implies disadvantages on both sides, on the one hand, the SSO Authentication Provider domain stores and handles user identities owned by Service Providers domains and, on the other hand, privacy of users and Service Providers is, at least, compromised.

[0016] Thereby, an important object of the present invention is the provision of means and methods for allowing that different user's identities of a user, the user's identities belonging to different domains, can be automatically linked and provisioned by both the SSO Authentication Provider and a Service Provider. It is another object of the present invention that, apart from maintaining the required security of users authentication, privacy of users and Service Providers is not compromised. It is a further object of the present invention to provide a mechanism for users accessing a Service Provider in an anonymous manner after having been authenticated in an SSO Authentication Provider domain, the mechanism in conformity with the means and methods of the above objects.

SUMMARY OF THE INVENTION

[0017] To accomplish the above objects, and other advantages, there is provided in accordance with the invention a method of providing Single Sign-On services to a user accessing at least one Service Provider, the user having a number of local user identities for accessing a number of Service Providers. This method comprising a step of authenticating the user at an Authentication Provider with a user identity used for authentication purposes; and further comprising the steps of:

- assigning at the Authentication Provider a temporary alias identity to the user for the first time the user access the said at least one Service Provider identified by a given Service Provider identifier;

- linking, on permanent basis if allowed by the user or on temporary basis otherwise, respective user identities at the Authentication Provider and at the said at least one Service Provider, both sharing and uniquely exchanging the alias identity to identify the user at respective sites; and

- for a next time the user access the said at least one Service Provider, identifying the user by the shared alias identity if permanent linking was allowed by the user, or repeating the step of assigning a temporary alias identity to the user otherwise.

[0018] In this method, the step of linking respective user identities on permanent or on temporary basis includes a step of checking corresponding user's preferences at an Authentication Provider user's profile, and a step of asking the user for a local identity and password to identify the user locally at the Service Provider. An

important advantage is obtained with this method applied for a user not having yet an account with the Service Provider, the user selecting a local identity and password, and the Service Provider registering a new account for the user with said Service Provider.

[0019] Moreover, the above step of linking respective user identities on permanent basis includes a step of linking at the Authentication Provider the user identity used for authentication purposes, the assigned alias identity and a given identifier of the Service Provider where the user accesses; and a step of linking at the Service Provider, where the user accesses, the local user identity and the alias identity assigned.

[0020] Another additional advantage is obtained, in case accessing users may be authenticated with different Authentication Providers, when the step of linking the local user identity and the alias identity at the Service Provider also comprises a step of linking an identifier of the Authentication Provider in charge of each user.

[0021] Apart from the above method, there are provided an Authentication Provider and a Service Provider arranged in accordance with the invention to accomplish the above objects and other advantages.

[0022] The Authentication Provider arranged for carrying out a Single Sign-On authentication of a user accessing at least one Service Provider, and arranged for returning an authentication token or artefact to the user as a result of the authentication, the user having a user's identity used for authentication purposes. This Authentication Provider comprising:

- means for assigning a temporary alias identity to the user, for the first time the user access the said at least one Service Provider identified by a given Service Provider identifier; and

- means for linking the user identity used for authentication purposes, with the assigned alias identity and the given identifier of the Service Provider where the user accesses.

[0023] An advantageous Authentication Provider comprises a Session Manager having means for checking if a user identified by a user's authentication identity has an active session, means for checking if there is a shared alias identity for the user with a session in a Service Provider, and means for ordering the generation of an authentication assertion with said shared alias identity for the user. This advantageous Authentication Provider also comprises a Security Assertion Mark-up Language (SAML) engine having means for generating an authentication assertion with a shared alias identity for a user.

[0024] Additional advantages may be obtained by having an Authentication Provider that comprises an Identity Manager having means for determining whether a shared alias identity exists for a user in a Service Provider, means for assigning a new shared alias identity for said user, and means for linking a shared alias identity for the user in a Service Provider with an identifier of said Service Provider and with a user's authentication identity. Moreover, this Identity Manager having further means for determining user's preferences for a user in respect of linking user's identities.

[0025] Further advantages may be obtained from this Authentication Provider by having therein a user's profile

directory (6) with storage for linking user's identities with identifiers of Service Providers.

[0026] The Service Provider, in accordance with the invention, having means for receiving a service request from an accessing user, the service request including an authentication artefact for the user, means for verifying the authentication artefact with an Authentication Provider having generated the artefact, and means for obtaining from a user a local user's identity to identify a user's account with the Service Provider. The Service Provider comprising:

- means for obtaining from an Authentication Provider a shared alias identity for the user; and

- means for linking the local user's identity with the received shared alias identity.

[0027] An additional advantage is obtained, in case the accessing users may be authenticated with different Authentication Providers, with the Service Provider further comprising means for linking an identifier of the Authentication Provider with the local user's identity and with the received shared alias identity.

[0028] Further additional advantages are obtained with this Service Provider comprising means for registering a new user's account with the Service Provider for a user not having a local user's identity assigned to any account with the Service Provider.

[0029] In both, the above apparatus and method, a user is identified between an Authentication Provider and a Service Provider with a shared identity, independently of the authentication identity used between the user and the Authentication Provider, and independently of the user identity used between the user and the Service Provider.

BRIEF DESCRIPTION OF DRAWINGS

[0030] The features, objects and advantages of the invention will become apparent by reading this description in conjunction with the accompanying drawings, in which:

[0031] **FIG. 1** schematically represents a Single Sign-On scenario in which users manually input their specific user identity per service provider into an authentication provider's database.

[0032] **FIG. 2** shows a simplified sequence diagram representing the process of linking identities between a Service Provider and an SSO Authentication Provider in accordance with an aspect of the invention.

[0033] **FIG. 3A** shows another simplified sequence diagram representing the process followed in accordance with an embodiment of the present invention to authenticate a user having a user's identity for authentication purposes in an authentication provider.

[0034] **FIG. 3B-3C** illustrate an exemplary process of linking identities between a Service Provider and an SSO Authentication Provider in accordance with another embodiment of the present invention.

[0035] **FIG. 4** shows an exemplary process for identity selection during a user's authentication carried out at a corresponding Authentication Provider site in accordance with an embodiment of the invention.

[0036] **FIG. 5** illustrates an exemplary generation of a user's Temporary Identity for an anonymity service during a user's authentication carried out at a corresponding Authentication Provider site in accordance with an embodiment of the invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0037] The following describes currently preferred embodiments of means, and methods for handling, provisioning and correlating a plurality of user identities for a user in an automated manner between an SSO Authentication Provider and a number of Service Providers in order to allow each user having a personalised access, including anonymous access, to said Service Providers where each user already has, or can register, an account.

[0038] Therefore, in accordance with a first aspect of the present invention, a user is identified between an Authentication Provider and a Service Provider by a shared identity, independently of an authentication identity used between the user and the Authentication Provider, and independently of a user identity used between the user and the Service Provider.

[0039] In accordance with a second aspect of the present invention, a Mobile Network Operator (MNO) may act as an SSO Authentication Provider for its own subscribers towards other Service Providers having such agreement with the Mobile Network Operator. In accordance with a third aspect of the invention, a first Service Provider capable of performing an SSO authentication may act as an SSO Authentication Provider towards a number of second Service Providers accepting such SSO authentication from said first Service Providers for a number of users.

[0040] One important feature that the present invention is based on is the linking of user identities between an SSO Authentication Provider and a Service Provider where a user is accessing. A first step prior to this identity linking is an authentication of the user with said SSO Authentication Provider. This authentication may be carried

out by different mechanisms suitable for Single Sign-On as well as for other services inasmuch as the user obtains a token as a result. The token may be, for example, a Security Assertion Mark-up Language (SAML) artefact, a Passport cookie, a Kerberos token, or others.

[0041] Once the user has been authenticated by an SSO Authentication Provider and has thus obtained from the SSO Authentication Provider (SSO AP) an authentication token or artefact, a sequence of actions take place in order to appropriately link different user identities at different entities to achieve the objects of the invention.

[0042] Under a currently preferred embodiment of the invention illustrated in Fig. 2, the user presents (S-541) the token to a Service Provider (SP-2) where the user (5) requests access. This token comprises an implicit reference to the user (user Ref.) that is preferably understood only by the SSO Authentication Provider (SSO AP). Given that the Service Provider (SP-2) needs authenticate this user (5), the Service Provider (4) sends (S-411) an authentication query toward the SSO Authentication Provider (SSO AP) (1) to authenticate the user. The Service Provider (4) includes the reference to the user (user Ref.) received in the token along with an identifier of the Service Provider (SP_name).

[0043] The SSO AP (1) receiving such authentication request fetches a user's internal identity at the Authentication Provider, namely a user's identity for authentication purpose (AP_ID), and then searches in the user's profile (6) for an identity-entry corresponding to the requester Service Provider (SP_name). Given that no identity-entry exists in the user's profile yet since identity linking has not been performed, the SSO AP (1) generates a temporary alias identity (ALIAS_ID) for identifying the user (5). This step avoids revealing the

user's identity used for authentication (AP_ID) to the Service Provider (4). In this manner, both the Service Provider (4) and the SSO Authentication Provider (1) refer to the user with said temporary alias identity (ALIAS_ID).

[0044] The SSO AP thus confirms the user's authentication with an authentication response (S-141) to the Service Provider having issued the query, the response including the temporary alias identity (ALIAS_ID). The Service Provider (SP-2) only has knowledge of this identity, and hence it is not aware that it is in fact an alias.

[0045] Then, the Service Provider (4) searches (S-471) in its local database (7) for any entry corresponding to the received user identity, namely the temporary alias identity (ALIAS_ID) in this case. As a permanent identity linking has not been performed yet, no entry exists for this identity and the temporary alias identity (ALIAS_ID) is reported (S-741) as unknown. The Service Provider (4) asks (S-451) the requester user (5) for its local identity (SP_ID) and password, which is valid for said Service Provider (4) site basis to authenticate the user locally when the user already has an account with the Service Provider. Upon receipt (S-542) of the user's local identity (SP_ID) and password, such local authentication takes place at the Service Provider. If the user does not have an account it may register for one at this point. This is an additional advantage of this mechanism wherein an on-line registration of a new account can be triggered while carrying out the identity linking process.

[0046] At this stage, the Service Provider (4) requests permission (S-412) from the SSO Authentication Provider (1) to link identities locally indicating the temporary alias identity (ALIAS_ID) to be linked. This type of query may be rather expressed in terms of co-ordination of respective

linking actions between the SSO Authentication Provider (1) and the Service Provider (4). This step is advantageous in order to avoid that a Service Provider links user identities without explicit consent of the user expressed in the corresponding user profile at the Authentication Provider.

[0047] The SSO Authentication Provider consults (S-161) the user's profile to check if said user (ALIAS_ID) has allowed an identity linking at the Service Provider (SP-2) accessed by the user and identified by a given identifier (SP_name). This might be the case where users specify that identity linking should not occur at certain web sites such as adult content sites. At present, if the user has allowed identity linking for the given Service Provider (4), the SSO Authentication Provider updates the user's profile with such user's identity (ALIAS_ID) for the given Service Provider (SP-2) identified by a given identifier (SP_name). The user's profile (6) responds (S-611) with a successful message once the updating has been validly completed, and the SSO Authentication Provider (1) in its turn authorises (S-142) the link operation to the Service Provider (4) having respective link of identity awaiting co-ordination. At this point, the previously considered temporary alias identity can be rather considered a shared identity between the Service Provider and the Authentication Provider.

[0048] The Service Provider (4) inserts in its local user's profile the shared identity (ALIAS_ID) along with the user's local identity (SP_ID), which is valid and preferably only known by said Service Provider (4). The Service Provider (4) eventually grants access to the user (5), and from now on it will greet the user with the user's local identity (SP_ID) and the user's account.

[0049] These set of actions described above preferably occurs just once when a user accessed a Service Provider at the first time and a token is presented to an SSO Authentication Provider. A next time the user presents a token requesting access to this Service Provider (4), the SSO Authentication Provider (1) authenticates the user's shared identity (ALIAS_ID) for the identifier (SP_name) of said Service Provider as found in the user's profile (6) where the user is internally known by its authentication identity (AP_ID) for which its authentication status can be checked. Then, the Service Provider (4) queries its local user profile database (7) with the shared identity (ALIAS_ID), for which a permanent rather than temporary link has been established, and obtains the local user's identity (SP_ID). After this, the Service Provider grants access to the user with its local user's identity (SP_ID) in a customised manner.

[0050] The solution described above and illustrated in Fig. 2 is also applicable and thus solves privacy and identity concealment. This is achieved by the transitory property of the temporary alias identity (ALIAS_ID) generated by the SSO Authentication Provider. In accordance with the above description, if a user does not wish to link permanently its user's identities at certain Service Providers said user may have blacklisted under the SSO Authentication Provider premises a number of web sites. In this case, upon request (S-412) for permission to link user's identities from a Service Provider (4), the SSO Authentication Provider (1) answers with a Deny Link Operation. With this denial, the temporary alias identity (ALIAS_ID) is merely temporary populated in the user's profile (6) at the Authentication Provider side for the given Service Provider (4), or even not populated at all and simply cached for a while. At this stage, it is noticed

that the user would most probably skip those steps illustrated in figure 2 for providing a local identity (SP_ID) and for registering an account with the Service Provider.

[0051] In accordance with the invention there is provided a mechanism whereby user's identities can be unlinked. Therefore, a similar mechanism as the one shown in Fig. 2 takes place with a new authorisation query (S-411) to indicate the Unlinking of identities. Further accesses by the user to the same Service Provider (4) result in a temporary alias identity (ALIAS_ID) to be assigned by the SSO Authentication Provider (1). If the Service Provider requests (S-412) authorisation to Link Identities after having requested the unlinking, the SSO Authentication Provider (1) responds with a deny result.

[0052] Under the above embodiment the concept of shared alias identity (ALIAS_ID) was introduced with the intention of being an identity that univocally and simultaneously identifies a user to an SSO Authentication Provider and to a Service Provider. The SSO Authentication Provider is thus able to correlate the shared alias identity (ALIAS_ID) with the user's identity used for authentication (AP_ID) for a user, whereas the Service Provider is able to correlate the shared alias identity (ALIAS_ID) with a local user's identity (SP_ID) for said Service Provider.

[0053] At this point certain considerations may be taken into account depending on the value of a user's alias identity (ALIAS_ID). The user's alias identity (ALIAS_ID) may adopt the same format and value for all the Service Providers the user might access to, or might adopt a different format or value for different Service Providers.

[0054] The case of adopting a different format or value for different Service Providers has the snag of resulting in high-cost search operations in the user's profile directory (6) when a different user's alias identity per service provider is used to perform the search. It might be preferable in this case to first map the alias identity (ALIAS_ID) to the user's authentication identity (AP_ID) and perform the search with this identity. However, this is apparently feasible only if this correlation is maintained elsewhere, for example, in a Session Manager database as other preferred embodiments suggest as shown in Fig. 3A-3C Fig. 4 and Fig. 5. The Session Manager may correlate a shared alias identity (ALIAS_ID) with the authentication identity (AP_ID) for existing sessions. The Session Manager could also store this correlation temporarily in a local cache even after a session is over. This allows a Service Provider to originate queries concerning a shared alias identity (ALIAS_ID) during or shortly after a session with a resulting low-cost search operation in the user's profile directory (6) at the authentication Provider site. On the other hand, once the alias identity (ALIAS_ID) has been removed from the session manager and local cache, there is no alternative for the Authentication Provider but to search in the user's profile directory with the alias identity (ALIAS_ID). For instance, when a Service Provider wishes to check with the Authentication Provider certain information concerning many users with respective alias identities off-line.

[0055] The case of a user's alias identity (ALIAS_ID) adopting a the same format and value for all the Service Providers simplifies the search in the Authentication Provider user's profile directory. Such directory lookup operation would be comparable to performing a lookup based on the user's authentication identity (AP_ID) and should

not be as costly search-wise as for the previous case. A snag with this approach is the possible ability of Service Providers to carry out a so-called "profile sharing" based on the user's alias identity (ALIAS_ID) without the user's consent. This identity is likely common to a number of Service Providers so that it would be possible for a given Service Provider to query another Service Providers about a certain user identified by said common user's alias identity (ALIAS_ID).

[0056] In short and according to another aspect of the present invention, the practitioner may choose between having a user's alias identity (ALIAS_ID) with the same format and value for all the Service Providers, or having different user's alias identities for different Service Providers, without being away from the teachings behind the invention.

[0057] Thus, the user's identities linking is the process of correlating user's identities at both the Authentication Provider and a number of Service Providers, and particularly oriented to offer effective Single Sign-On services. Initial conditions for identity linking may be established by a SAML authorisation assertion and embedded in processes of accessing a service provider. In this respect and in accordance with another preferred embodiment of the present invention, Fig. 3A-3C describe the steps appropriate to perform an identity linking via a SAML engine.

[0058] As already commented above in respect of the embodiment illustrated in Fig. 2, a first step prior to the identity linking is an authentication of the user at said SSO Authentication Provider in order to obtain a token or artefact. Fig. 3A illustrates an embodiment of this user authentication at an SSO Authentication Provider (SSO AP)

which in the present case comprises a Session Manager (8) and an Identity Manager (9). The SSO AP (1; 8, 9) is complemented with an Authentication Provider user's profile directory (6) which may be included in, or in communication with, the SSO AP in both embodiments respectively illustrated in Fig. 2 and Fig. 3A-3C.

[0059] For the sake of clarity, the already introduced concept of user's alias identity (ALIAS_ID) per Service Provider, which may be linked on either permanent or temporary basis, is replaced under this embodiment by two identity names to better differentiate whether the linking is permanent or temporary, though said two identity names may be particularly the same. That is, the term Temporary Identity (TMP_ID) refers to a temporary linked user's alias identity (ALIAS_ID) under this embodiment, whereas the term Shared Identity (SHARED_ID) refers to a permanently linked user's alias identity (ALIAS_ID). Moreover, the term Temporary Identity (TMP_ID) might be understood as an implicit reference to the user (user Ref.) presented under the embodiment of Fig. 2, especially in the case that Temporary Identity (TMP_ID) and Shared Identity (SHARED_ID) are not the same identity.

[0060] In accordance with the embodiment in Fig. 3A, a user (5) requests authentication (S-581) toward the SSO AP (8, 9) via a Session Manager (8). The Session Manager receiving such authentication request queries (S-891) an Identity Manager (9) device about a user's Shared Identity (SHARED_ID) for the Service Provider (4) where the user (5) has accessed. It must be noticed that the Authentication Provider (1; 8, 9) receives the user's identity for authentication purposes (AP_ID) as well as an identifier of said Service Provider (SP_name) where the user has accessed. Given that this is the first time the user

accesses this Service Provider site via Single Sign-On authentication, there is no user's Shared Identity (SHARED_ID) yet for the requested site (SP_name). Hence, when the Identity Manager (9) sends (S-961) a query to the Authentication Provider (hereinafter AP) user's profile (6), such query returns (S-691) a response indicating no entry found. Then, the Identity Manager (9) generates a Temporary Identity (TMP_ID) for the user (5) and correlates it to both the user's authentication identity (AP_ID) and to the identifier (SP_name) of the Service Provider (4) accessed by the user. This correlation may be stored locally by the Identity Manager until either the Temporary Identity (TMP_ID) expires, or identities are permanently linked, in the latter case the Temporary Identity becomes a user's shared identity (SHARED_ID). As a result, an authentication assertion is generated by the Authentication Provider and returned back (S-851) to the Service Provider, namely an authentication artefact, said artefact populated with the Temporary Identity (TMP_ID).

[0061] After having presented an embodiment of the prior authentication, a further embodiment for identity linking is described with reference to Fig. 3B and Fig. 3C. This further embodiment provides for having a SAML engine (8a) in co-operation with, or replacing, the above Session Manager (8) for handling assertions for a given user and for a specific destination side, which in the present case may be the Service Provider (4) site.

[0062] As shown in Fig. 3B, the user (5) presents (S-541) the obtained authentication artefact to the Service Provider (4) where the user accesses. The Service Provider sends (S-48a1) an Authentication Request message to the SSO AP, for example, via a SAML engine (8a), and based on information received in the artefact. The SAML engine (8a)

in co-operation with, or replacing, the above Session Manager (8) responds (S-8a41) with the previous authentication assertion generated for the user's Temporary Identity (TMP_ID). Then, the Service Provider (4) receiving such assertion extracts the user's Temporary Identity (TMP_ID) element from the assertion and lookups (S-471) in its local user profile directory (7) returning back (S-741) an answer of type identity unknown. At this point, the Service Provider asks (S-451) the user for a local identity (SP_ ID) and password to authenticate the user locally in case it already has an account at said Service Provider.

[0063] Upon provision (S-542) of local identity (SP_ ID) and password from the user, Fig. 3C shows that the Service Provider (4) authenticates (S-441) the user locally. In the case the user does not have a valid account at this Service Provider, a new account can be registered at this point in accordance with another aspect of the present invention.

[0064] Then, the Service Provider (4) sends a SAML authorisation query (S-48a2) for requesting permission to link identities locally toward the Authentication Provider (8, 9; 8a, 9) via the SAML engine (8a). The query includes the Temporary Identity (TMP_ID) previously received and temporary linked, likely in a local cache. This request of permission may be substituted by a sort or co-ordination between both sites without affecting substantially the scope of the invention. This type of query may be defined via a SAML Authorisation Decision Query with an action field set to indicate linking.

[0065] The SAML engine (8a) at the Authentication Provider receives the SAML query and invokes (S-8a91) the Identity Manager (9) to handle the current identity linking process. The Identity Manager (9) checks the user's profile directory (6) with the user's authentication identity

(AP_ID) to see whether corresponding user preferences allow a permanent identity linking with the currently accessed Service Provider (4) or not. If the user's preferences allow such permanent linking, either the Temporary Identity (TMP_ID) becomes the Shared Identity (SHARED_ID), or another Shared Identity (SHARED_ID) different from the Temporary Identity (TMP_ID) is seized to this end. This Shared Identity (SHARED_ID) is submitted (S-962) to the AP user's profile directory (6) in order to be linked therein with the identifier (SP_name) of the Service Provider (4), and with the user's authentication identity (AP_ID). Once such linking has been updated (S-692) in the AP user's profile directory (6), a corresponding linking action is indicated (S-98a1) from the Identity Manager (9) to the SAML engine (8a). In addition, the Identity Manager takes necessary actions for deleting the previous Temporary Identity (TMP_ID) from its local cache, or thus indicates to do toward the user's profile directory (6) in case the temporary linking was carried out therein. The SAML engine responds (S-8a42) to the previous authorisation query from the Service Provider (4) with an authorisation assertion indicating whether identity linking is allowed and, when allowed, including the identity to be linked (SHARED_ID).

[0066] The Service Provider (4), on reception (S-8a42) of such linking indication, submits (S-472) the new received user's Shared Identity (SHARED_ID) toward its user's profile directory (7) for linking said Shared Identity with the corresponding user's local identity (SP_ ID) at said Service Provider (4). In addition, the Service Provider takes proper actions for deleting the previous Temporary Identity (TMP_ID) from its local cache, or thus indicate to do toward the user's profile directory (7) in case the temporary linking was carried out therein. Once the Service Provider (4) receives (S-742) a successful result of the

linking operation from its user's profile directory (7), the user is granted access to the Service Provider (4), the latter greeting the user with the user's local identity (SP_ID) and account.

[0067] This embodiment commented above in respect of Fig. 3A-3C preferably occurs only for the first time a user (5) accesses a Service Provider (4) via a Single Sign-On (SSO) authentication. In accordance with the invention, the next time the user accesses the same Service Provider (4), the SSO Authentication Provider (1, 6; 8, 9, 6; 8a, 9, 6) generates an assertion with a shared alias identity (ALIAS_ID; SHARED_ID) populated as a function of the Service Provider (4) accessed by the user. Thanks to this shared alias identity, anonymity of user is achieved between service provider domain and authentication provider domain.

[0068] An advantageous embodiment of another aspect of the present invention is illustrated in Fig. 4 wherein an identity selection process is carried out at an Authentication Provider site (1, 6; 8, 8a, 9, 6) for a user (5) being authenticated.

[0069] As shown in Fig. 4, a user (5) requests (S-581) authentication by including a user's identity for authentication purposes (AP_ID) in order to further get a granted access to a selected service provider. The Session Manager (8) receiving said request invokes an Identity Manager (9) by asking (S-891) for a Shared Identity (SHARED_ID) with the received user's authentication identity (AP_ID) and with an identifier (SP_name) of the selected Service Provider. The Identity Manager (9) queries (S-961) its user's profile directory (6) in order to retrieve (S-693) a Shared Identity (SHARED_ID) for said user at the selected Service Provider. The Identity Manager

returns back (S-982) the Shared Identity (SHARED_ID) to the Session Manager (8). At this point, the Session Manager sends (S-88a1) said Shared Identity (SHARED_ID) to a SAML engine (8a) for the latter generating an assertion with the received Shared Identity (SHARED_ID). This assertion, also called artefact for the purpose of the present invention, is returned (S-8a81) to the requester Session Manager which, in turn, sends it back (S-851) to the user as a successful authentication result.

[0070] Under this embodiment the Session Manager (8) correlate a user's set of Shared Identities (SHARED_ID) with identifiers (SP_name) of a corresponding number of Service Providers currently in use throughout a session and a user's authentication identity (AP_ID). This allows for lookups to be done based on said user's authentication identity (AP_ID).

[0071] Still another advantageous embodiment of another aspect of the present invention is illustrated in Fig. 5 wherein a generation of a user's Temporary Identity (TMP_ID) for an anonymity service is carried out at an Authentication Provider site (1, 6; 8, 8a, 9, 6) for a user (5) being authenticated. Under this embodiment there is provided a solution to cater for anonymity wherein a user (5) wishes to access a Service Provider in an anonymous mode, that is, have a property set to Conceal, and said property populated in the user's profile. The Identity Manager (9) interprets this property and generates a Temporary Identity (TMP_ID) for the user (5) to be used and preferably stored by the Session Manager.

[0072] In accordance with the flow depicted in Fig. 5, a user (5) requests authentication (S-581) for a specific service provider and furnishes his user's authentication identity (AP_ID) to a Session Manager (8) at the

Authentication Provider site. The Session Manager checks user sessions and requests (S-891) fetching a user's Shared Identity (SHARED_ID) for the specific service provider toward an Identity Manager (9). The Identity manager searches (S-961) its user's profile directory (6) to fetch the user's Shared Identity (SHARED_ID) for the specific service provider. In the present case, user's preferences indicate (S-694) that an identity concealment service has been requested by the user for accessing said specific service provider. Then, the Identity Manager (9) generates (S-991) a user's Temporary Identity (TMP_ID) for said specific service provider, and the Identity Manager (9) stores said user's Temporary Identity (TMP_ID) locally in its local cache with a specified time-to-live value (TTL).

[0073] Next, the Identity Manager returns (S-981) said user's Temporary Identity (TMP_ID) back to the Session Manager (8). The Session Manager forwards (S-88a1) the user's Temporary Identity (TMP_ID) to the SAML engine (8a) for the latter to create an assertion based on said user's Temporary Identity (TMP_ID). As a result an authentication artefact is returned (S-8a81) to the Session Manager which, in turn, returns (S-851) such authentication artefact to the user.

[0074] Thus, under this embodiment, the Identity Manager assumes the responsibility of generating a Temporary Identity for the user and storing such Temporary Identity locally to be used throughout the session. The Time-To-Live value of this Temporary Identity (TMP_ID) may be specified in advance, or subject to Session Manager premises. In other words, once a user has finished a session the Session Manager instructs the Identity Manager to delete a user's Temporary Identity from the cache. In this case, the

Temporary Identity (TMP_ID) is not linked and does not become a Shared identity (SHARED_ID).

[0075] Applicant's invention is described above in connection with various embodiments that are intended to be illustrative and non-restrictive. It is expected that those of ordinary skill in this art may modify these embodiments. The scope of Applicant's invention is defined by the claims in conjunction with the description and drawings, and all modifications that fall within the scope of these claims are intended to be included therein.

CLAIMS

1. A method of providing Single Sign-On services to a user (5) accessing at least one Service Provider (4), the user having a number of local user identities (SP_ID-1, SP_ID-2) for accessing a number of Service Providers (SP-1, SP-2), the method comprising a step of:

(a) authenticating the user (5) at an Authentication Provider (1, 6) with a user identity used for authentication purposes (AP_ID);

the method **characterized by** comprising the steps of:

(b) assigning at the Authentication Provider (1, 6) a temporary alias identity (ALIAS_ID; TMP_ID) to the user for the first time the user access the said at least one Service Provider (4) identified by a given Service Provider identifier (SP_name);

(c) linking, on permanent basis if allowed by the user or on temporary basis otherwise, respective user identities at the Authentication Provider (1, 6) and at the said at least one Service Provider (4), both sharing and uniquely exchanging the alias identity (ALIAS_ID; TMP_ID; SHARED_ID) to identify the user (5) at respective sites; and

(d) for a next time the user (5) access the said at least one Service Provider (4), identifying the user by the shared alias identity (ALIAS_ID; SHARED_ID) if permanent linking was allowed by the user, or repeating the step of assigning a temporary alias identity (ALIAS_ID; TMP_ID) to the user otherwise.

2. The method of claim 1 wherein the step c) of linking respective user identities on permanent or on temporary basis includes a step of checking corresponding user's preferences at an Authentication Provider user's profile (6).

3. The method of claim 1 wherein the step c) of linking respective user identities includes a step of asking the user (5) for a local identity (SP_ID) and password to identify the user locally at the Service Provider (4).

4. The method of claim 3 wherein a user (5) not having yet an account with the Service Provider (4) can provide a selected local identity (SP_ID) and password to register an account with said Service Provider (4).

5. The method of claim 1 wherein the step c) of linking respective user identities on permanent basis includes the steps of:

(c1) linking at the Authentication Provider (1, 6) the user identity used for authentication purposes (AP_ID) with the assigned alias identity (ALIAS_ID; TMP_ID; SHARED_ID) and with the given identifier (SP_name) of the Service Provider (4) where the user (5) accesses; and

(c2) linking at the Service Provider (4) where the user (5) accesses the local user identity (SP_ID) with the alias identity (ALIAS_ID; SHARED_ID) assigned.

6. The method of claim 5 wherein the step c2) of linking the local user identity (SP_ID) and the alias identity (ALIAS_ID; SHARED_ID) at the Service Provider (4)

comprises a step of linking an identifier of the Authentication Provider (1; 8; 8a).

7. An Authentication Provider (1, 6; 8, 8a, 9, 6) arranged for carrying out a Single Sign-On authentication of a user (5) accessing at least one Service Provider (4), and arranged for returning an authentication token or artifact to the user as a result of the authentication, the user having a user's identity used for authentication purposes (AP_ID), the Authentication Provider **characterized in that** it comprises:

- means for assigning a temporary alias identity (ALIAS_ID; TMP_ID) to the user (5) for the first time the user access the said at least one Service Provider (4) identified by a given Service Provider identifier (SP_name); and

- means for linking the user identity used for authentication purposes (AP_ID) with the assigned alias identity (ALIAS_ID; TMP_ID; SHARED_ID) and with the given identifier (SP_name) of the Service Provider (4) where the user (5) accesses.

8. The Authentication Provider of claim 7, comprising a Session Manager (8) having means for checking if a user (5) identified by a user's authentication identity (AP_ID) has an active session, means for checking if there is a shared alias identity (ALIAS_ID; TMP_ID; SHARED_ID) for the user with a session in a Service Provider (4), and means for ordering the generation of an authentication assertion with said shared alias identity for the user.

9. The Authentication Provider of claim 8, comprising a Security Assertion Mark-up Language (SAML) engine (8a)

having means for generating an authentication assertion with a shared alias identity (ALIAS_ID; TMP_ID; SHARED_ID) for a user (5).

10. The Authentication Provider of claim 7, comprising an Identity Manager (9) having means for determining whether a shared alias identity (ALIAS_ID; TMP_ID; SHARED_ID) exists for a user (5) in a Service Provider (4), means for assigning a new shared alias identity (ALIAS_ID; TMP_ID) for said user (5), and means for linking a shared alias identity (ALIAS_ID; TMP_ID; SHARED_ID) for the user (5) in a Service Provider (4) with an identifier of said Service Provider (SP_name) and with a user's authentication identity (AP_ID).

11. The Authentication Provider of claim 10, comprising an Identity Manager (9) having means for determining user's preferences for a user (5) in respect of linking user's identities.

12. The Authentication Provider of claim 7, comprising a user's profile directory (6) having storage for linking user's identities (ALIAS_ID; TMP_ID; SHARED_ID; AP_ID) with identifiers of Service Providers (SP_name).

13. A Service Provider (4) having means for receiving a service request from an accessing user (5), the service request including an authentication artefact for the user, means for verifying the authentication artefact with an Authentication Provider having generated the artefact, and means for obtaining from the user a local user's identity (SP_ID) to identify a user's account with the Service Provider (4), the Service Provider **characterized in that** it comprises:

- means for obtaining from the Authentication Provider (1; 8a) a shared alias identity (ALIAS_ID; TMP_ID; SHARED_ID) for the user (5)

- means for linking the local user's identity (SP_ID) with the received shared alias identity (ALIAS_ID; TMP_ID; SHARED_ID).

14. The Service Provider of claim 13 further comprising means for registering a new user's account with the Service Provider for a user not having a local user's identity (SP_ID) assigned to any account with the Service Provider.

15. The Service Provider of claim 13 further comprising means for linking an identifier of the Authentication Provider (1; 8; 8a) with the local user's identity (SP_ID) and with the received shared alias identity (ALIAS_ID; TMP_ID; SHARED_ID).

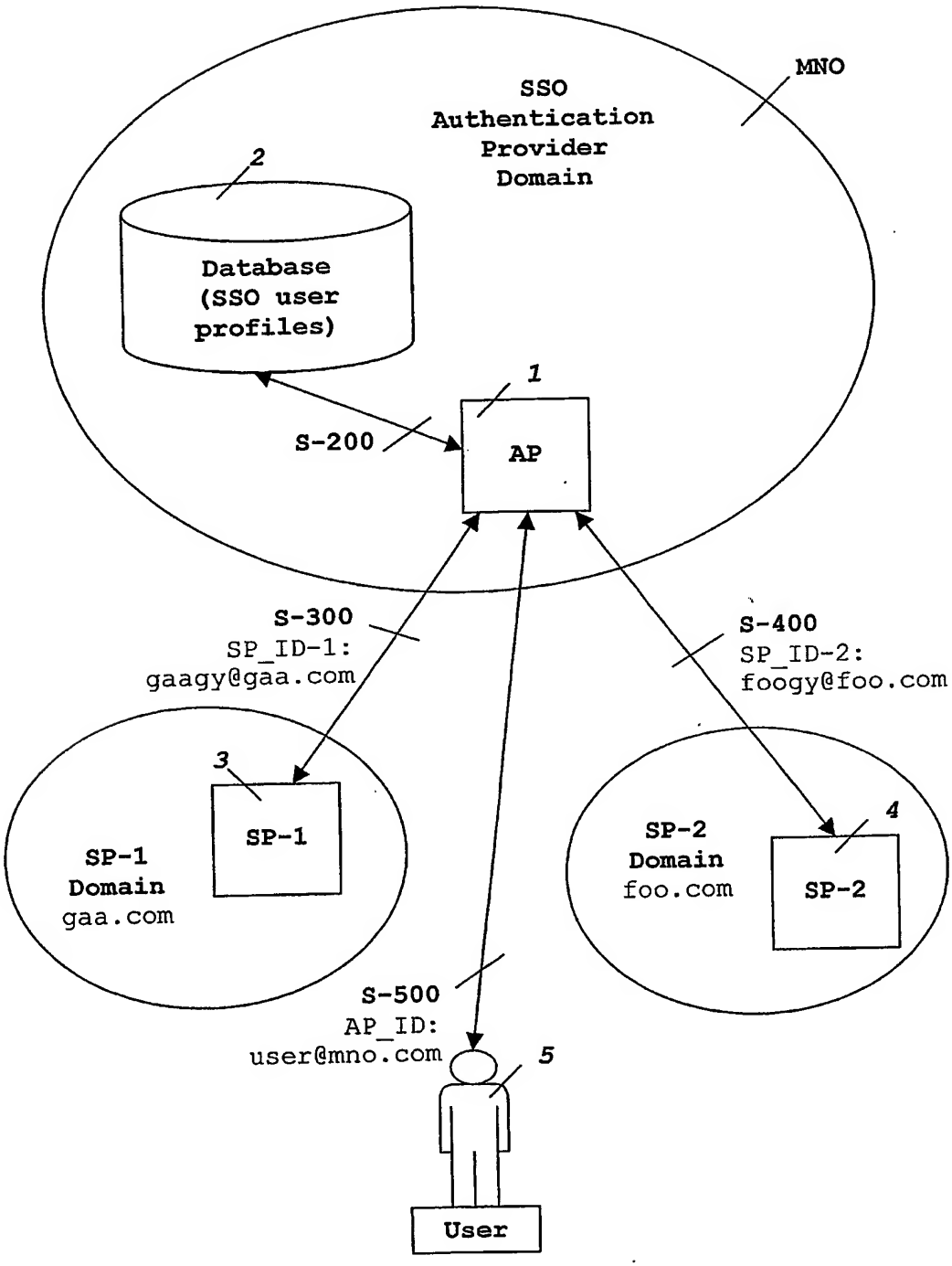


FIG.-1-
Related Art

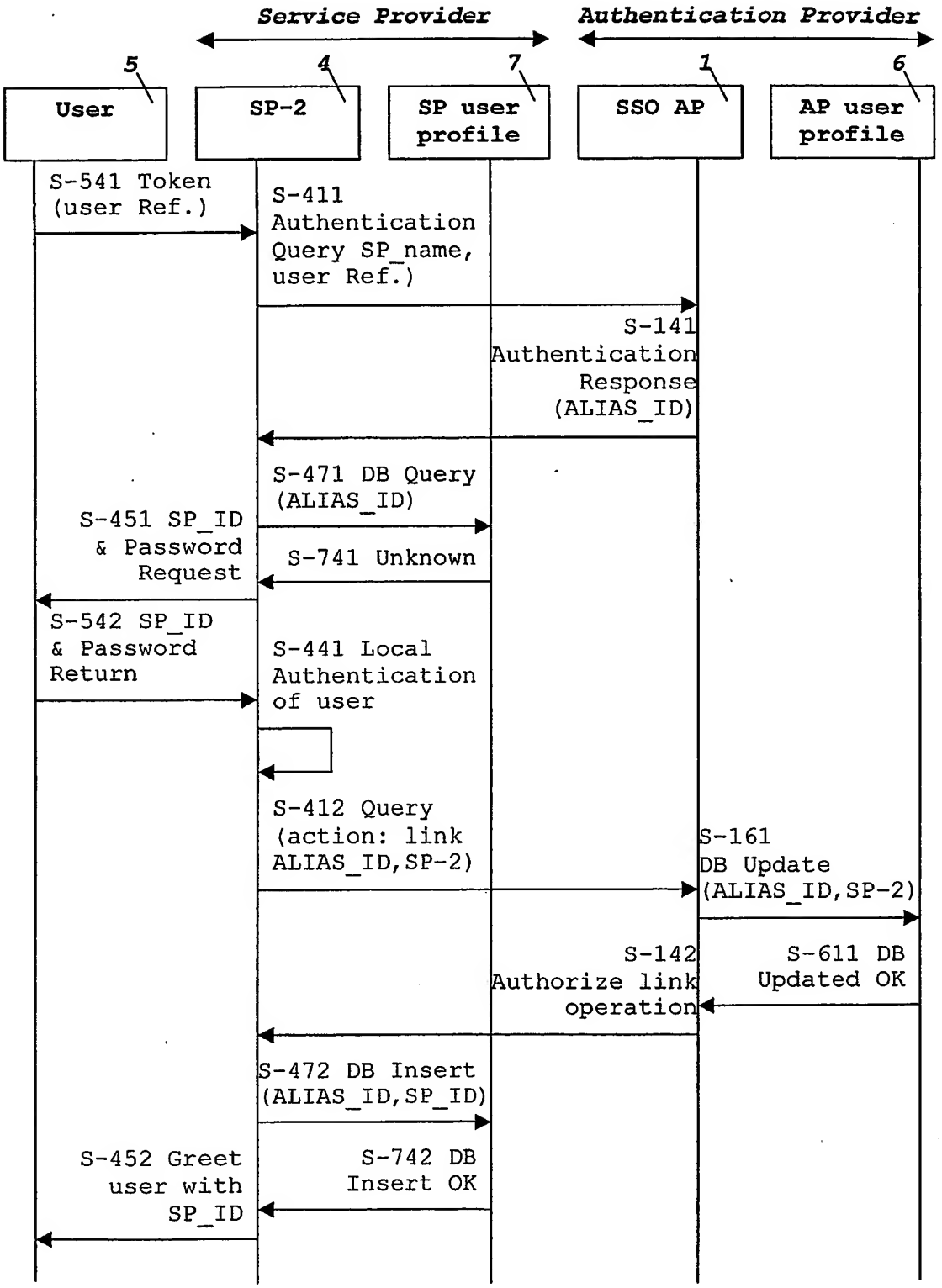

Service Provider
Authentication Provider
5
4
7
1
6
User
SP-2
SP user profile
SSO AP
AP user profile
S-541 Token (user Ref.)
S-411 Authentication Query SP_name, user Ref.)
S-141 Authentication Response (ALIAS_ID)
S-471 DB Query (ALIAS_ID)
S-451 SP_ID & Password Request
S-741 Unknown
S-542 SP_ID & Password Return
S-441 Local Authentication of user
S-412 Query (action: link ALIAS_ID,SP-2)
S-161 DB Update (ALIAS_ID,SP-2)
S-142 Authorize link operation
S-611 DB Updated OK
S-472 DB Insert (ALIAS_ID,SP_ID)
S-452 Greet user with SP_ID
S-742 DB Insert OK

FIG.-2-

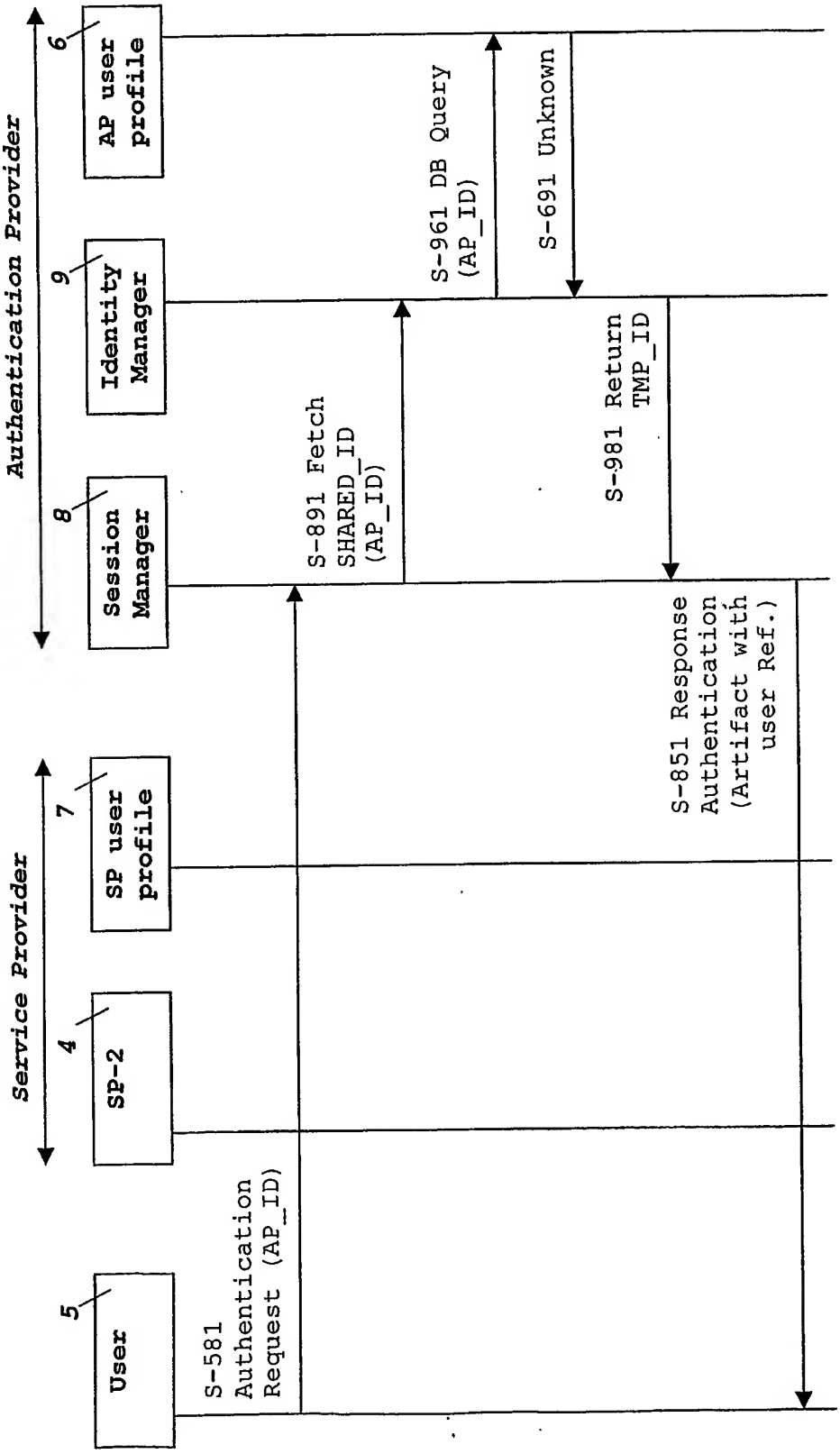

Authentication Provider
Service Provider
User
SP-2
SP user profile
Session Manager
Identity Manager
AP user profile
5
4
7
8
9
6
S-581 Authentication Request (AP_ID)
S-891 Fetch SHARED_ID (AP_ID)
S-961 DB Query (AP_ID)
S-691 Unknown
S-981 Return TMP_ID
S-851 Response Authentication (Artifact with user Ref.)

FIG.-3A-

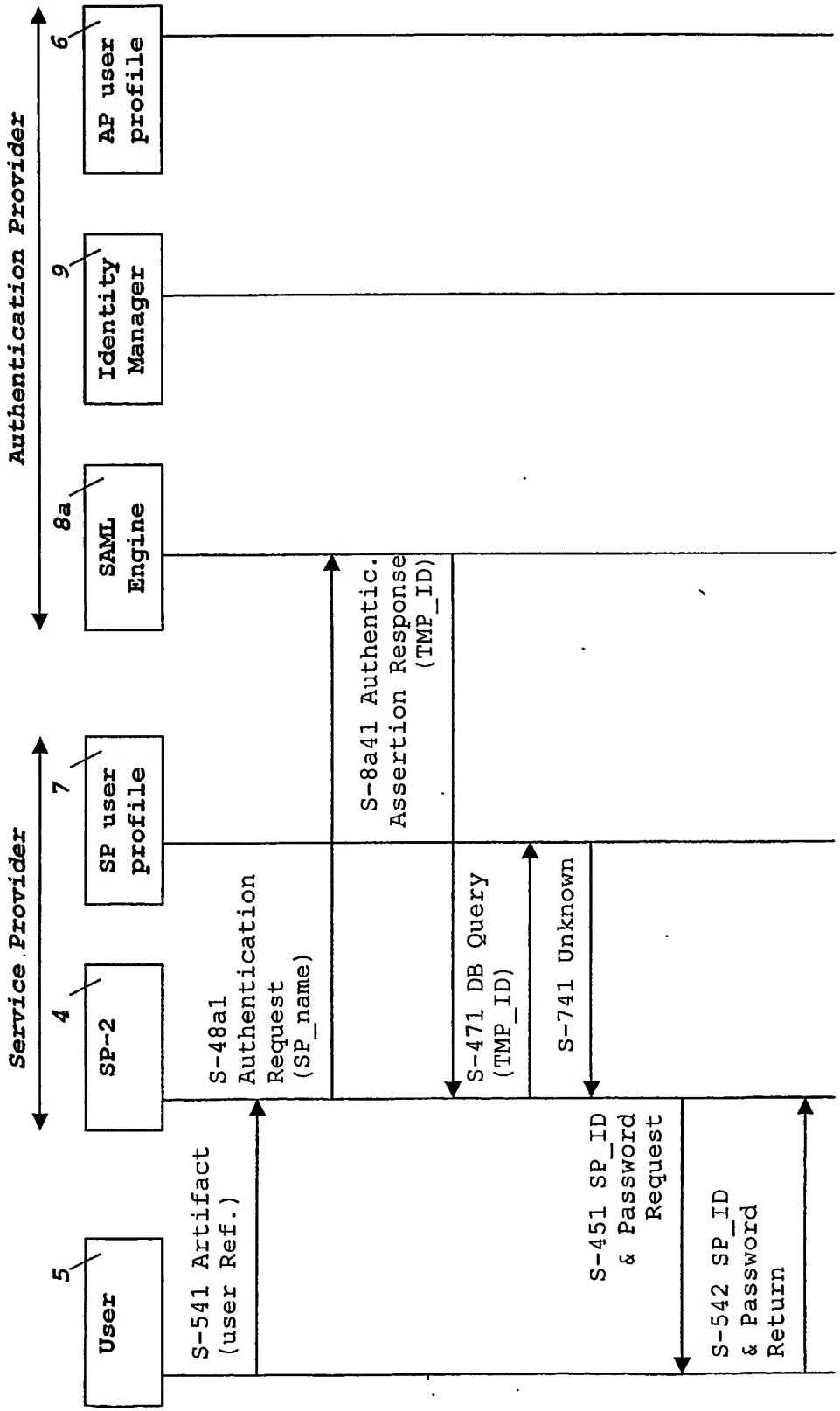

Service Provider
Authentication Provider
User
5
SP-2
4
SP user profile
7
SAML Engine
8a
Identity Manager
9
AP user profile
6
S-541 Artifact (user Ref.)
S-48a1 Authentication Request (SP_name)
S-8a41 Authentic. Assertion Response (TMP_ID)
S-471 DB Query (TMP_ID)
S-741 Unknown
S-451 SP_ID & Password Request
S-542 SP_ID & Password Return

FIG.-3B-

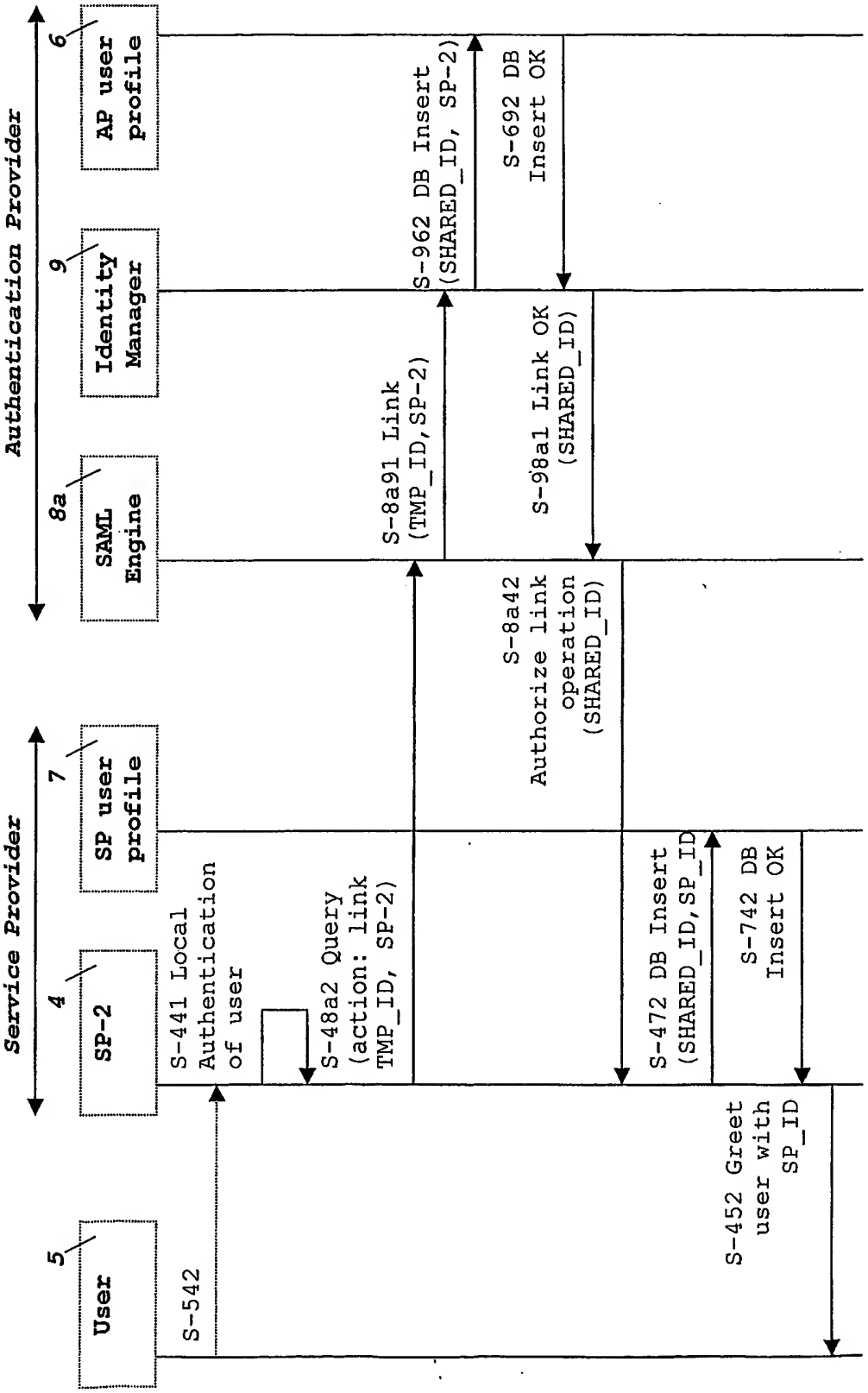

Authentication Provider
Service Provider
User
5
SP-2
4
SP user profile
7
SAML Engine
8a
Identity Manager
9
AP user profile
6
S-542
S-441 Local Authentication of user
S-48a2 Query (action: link TMP_ID, SP-2)
S-8a91 Link (TMP_ID,SP-2)
S-98a1 Link OK (SHARED_ID)
S-962 DB Insert (SHARED_ID, SP-2)
S-692 DB Insert OK
S-8a42 Authorize link operation (SHARED_ID)
S-472 DB Insert (SHARED_ID,SP_ID
S-742 DB Insert OK
S-452 Greet user with SP_ID

FIG.-3C-

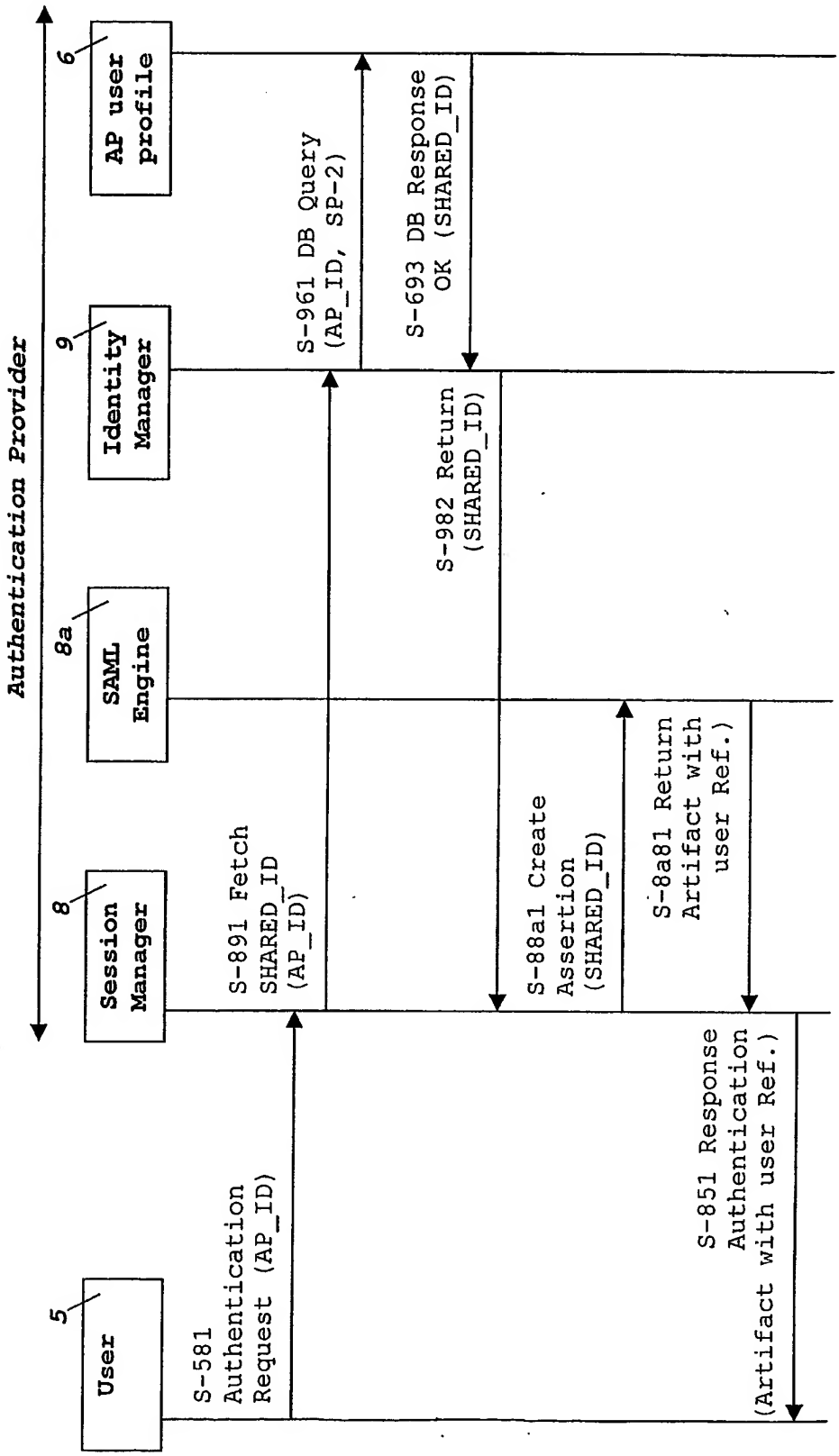

Authentication Provider
User
5
Session Manager
8
SAML Engine
8a
Identity Manager
9
AP user profile
6
S-581 Authentication Request (AP_ID)
S-891 Fetch SHARED_ID (AP_ID)
S-961 DB Query (AP_ID, SP-2)
S-693 DB Response OK (SHARED_ID)
S-982 Return (SHARED_ID)
S-88a1 Create Assertion (SHARED_ID)
S-8a81 Return Artifact with user Ref.)
S-851 Response Authentication (Artifact with user Ref.)

FIG.-4-

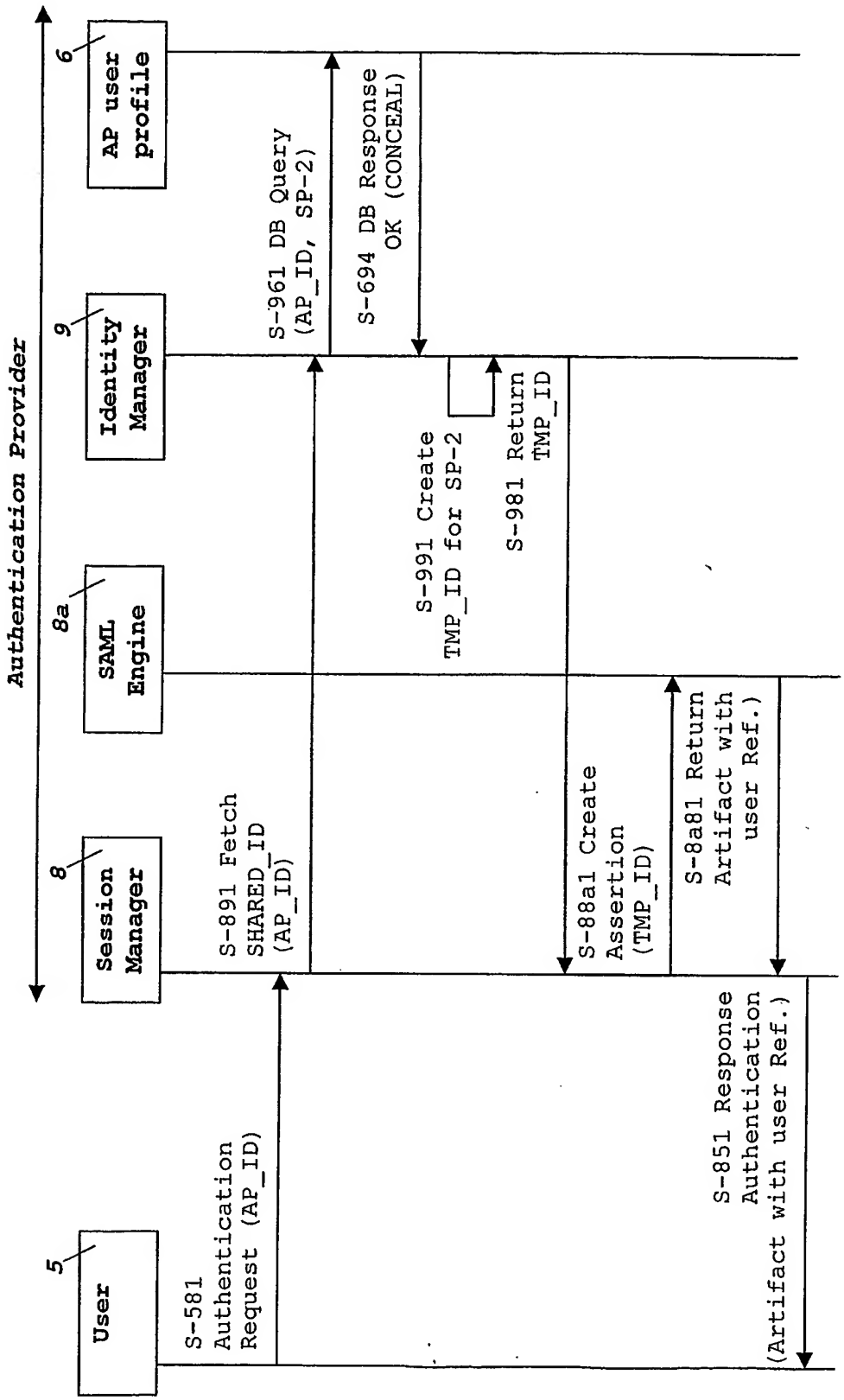

Authentication Provider
User
5
Session Manager
8
SAML Engine
8a
Identity Manager
9
AP user profile
6
S-581 Authentication Request (AP_ID)
S-891 Fetch SHARED_ID (AP_ID)
S-961 DB Query (AP_ID, SP-2)
S-694 DB Response OK (CONCEAL)
S-991 Create TMP_ID for SP-2
S-981 Return TMP_ID
S-88a1 Create Assertion (TMP_ID)
S-8a81 Return Artifact with user Ref.)
S-851 Response Authentication (Artifact with user Ref.)

FIG.-5-

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 03/00341

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01 72009 A (AT & T CORP) 27 September 2001 (2001-09-27) page 2, line 10 -page 3, line 16; claims 1-3; figures 1-4 abstract ---	1-15
A	EP 1 089 516 A (CITICORP DEV CT INC) 4 April 2001 (2001-04-04) paragraph (0006)-(0011) claim 1; figure 1 abstract ---	1-15
A	GB 2 349 244 A (VISAGE DEVELOPMENTS LIMITED) 25 October 2000 (2000-10-25) claim 1 abstract --- -/--	1-15

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date .

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 June 2003	09. 07. 2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	PÄR HEIMDAL /EÖ

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/SE 03/00341

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,A	US 6 421 768 B1 (PURPURA STEPHEN J) 16 July 2002 (2002-07-16) column 2, line 17 -column 3, line 3; figures 1,2 abstract ---	1-15
E	US 2003/061512 A1 (FLURRY GREGORY ALAN ET AL) 27 March 2003 (2003-03-27) paragraph (0014)-(0015) claim 1; figure 4 abstract -----	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/SE 03/00341

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0172009 A	27-09-2001	CA 2400623 A1	27-09-2001
		EP 1264463 A2	11-12-2002
		WO 0172009 A2	27-09-2001
EP 1089516 A	04-04-2001	CN 1289974 A	04-04-2001
		EP 1089516 A2	04-04-2001
GB 2349244 A	25-10-2000	AU 4604100 A	10-11-2000
		EP 1183583 A1	06-03-2002
		WO 0065424 A1	02-11-2000
US 6421768 B1	16-07-2002	AU 4983000 A	17-11-2000
		WO 0067415 A2	09-11-2000
US 2003061512 A1	27-03-2003	NONE	